1. A method of identifying a user, comprising the steps of:

a) selecting a modulus p from the group of equations consisting of:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r /= 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r /= 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r;$$

b) selecting an elliptic curve E and an order q;

c) selecting a basepoint G;

d) generating a private key w;

e) generating a public key $W=wG$;

f) distributing p, E, q, G, and W in an authentic manner;

g) retrieving, by a prover, the prover's private key w;

h) retrieving, by a verifier, the prover's public key W;

i) generating, by the prover, a private integer k;

j) combining, by the prover, k and the prover's G to form K using the form of the prover's modulus p;

k) sending, by the prover, K to the verifier;

l) sending, by the verifier, a challenge integer c to prover;

m) combining, by the prover, c, k, and w to form a response integer v;

n) sending, by the prover, v to the verifier; and

o) combining, by the verifier, cG, K, and W using the form of the prover's modulus p and checking to see if the combination is equal to vG, if so the user is identified as the user, otherwise the user is not identified as the user.

2. A method of generating a digital signature, comprising the steps of:

a) selecting a modulus p from the group of equations consisting of:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r /= 1, and where $GCD(c,d)$=1;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r /= 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r;$$

b) selecting an elliptic curve E and an order q;

c) selecting a basepoint G;

d) generating a private key w;

e) generating a public key $W=wG$;

f) distributing p, E, q, G, and W in an authentic manner;

g) retrieving, by a signer, the signer's private key w;

h) generating, by the signer, a private integer k;

i) combining, by the signer, k and G to form K using the form of the prover's modulus p;

j) combining, by the signer, K and a message M to form an integer h;

k) combining by the signer, h, k, and w to form an integer s; and

l) sending, by the signer, M and (K,s) as a digital signature of M.

3. The method of claim 1, further including the steps of:

a) retrieving, by the verifier, the prover's public key W;

b) receiving, by the verifier, M and (K,s);

c) combining, by the verifier, K and M to form an integer h; and

d) combining, by the verifier, h, k, and W using the form of the prover's modulus p and checking to see if the combination is equal to sG, if so then the digital signature is verified, otherwise the digital signature is not verified.

4. A method of generating a digital signature, comprising the steps of:

a) selecting a modulus p from the group of equations consisting of:

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $0<2c<=d$, where r /= 1, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\ldots-2^{k}+1)/r,$$

where d is even, and where k is not equal to 2 (mod 4);

$$p=(2^{dk}-2^{ck}-1)/r,$$

where $3d<6c<4d$, and where $GCD(c,d)=1$;

$$p=(2^{dk}-2^{ck}+1)/r,$$

where $0<2c<=d$, where r /= 1, and where $GCD(c,d)=1$; and

$$p=(2^{4k}-2^{3k}+2^{2k}+1)/r;$$

b) selecting an elliptic curve E and an order q;

c) selecting a basepoint G;

d) generating a private key w;

e) generating a public key $W=wG$;

f) distributing p, E, q, G, and W in an authentic manner;

g) retrieving, by a signer, the signer's private key w;

h) generating, by the signer, a private integer k;

i) combining, by the signer, k and G to form K using the form of the prover's modulus p;

j) combining, by the signer, K and a message M to form an integer h;

k) combining by the signer, h, k, and w to form an integer s; and

l) sending, by the signer, M and (h,s) as a digital signature of M.

5. The method of claim 4, further including the steps of:

a) retrieving, by the verifier, the prover's public key W;

b) receiving, by the verifier, M and (h,s);

c) combining, by the verifier, h, W, and sG using the form of the prover's modulus p to form K;

d) combining, by the verifier, K and M to form an integer h'; and

e) checking, by the verifier, that h is equal to h', if so then the digital signature is verified, otherwise the digital signature is not verified.